

1 This listing of claims will replace all prior versions, and listings, of claims
2 in the application:

3
4 **Listing of Claims**

5
6 Claim 1 (Original): A method comprising:

7 minting a stick of electronic assets by digitally signing with an issuer's
8 signature a composite of user-provided data items including a user identity, a
9 bottom asset from a bottom of the stick, and a length of the stick;

10 spending one or more assets from the stick at one or more vendors, wherein
11 each expenditure with a particular vendor involves digitally signing with a user's
12 signature a first asset from the stick to be spent and passing the user-signed first
13 asset along with the issuer-signed composite to the particular vendor for
14 verification and subsequently passing any additional assets to be spent without user
15 signature to the particular vendor; and

16 depositing one or more assets collected by the particular vendor by digitally
17 signing with the particular vendor's signature a composite of data items including
18 the user-signed first asset and a last asset spent by the user from the stick and
19 passing the vendor-signed composite along with the issuer-signed composite to the
20 issuer.

21
22 Claim 2 (Original): A method as recited in claim 1, further comprising
23 storing the stick of electronic assets in a tamper-resistant electronic wallet.

1 Claim 3 (Original): A method as recited in claim 1, further comprising
2 storing the stick of electronic assets in an electronic wallet constructed with a
3 secure-processor architecture.

4
5 Claim 4 (Original): A method as recited in claim 1, wherein the minting
6 comprises minting the stick of assets using a blind signature protocol.

7
8 Claim 5 (Original): A method as recited in claim 1, wherein the spending
9 comprises:

10 concatenating a vendor identity with the first asset from the stick to form a
11 payment request;

12 signing the payment request with a signature of the user;

13 submitting the user-signed payment request along with the issuer-signed
14 withdrawal request to the vendor;

15 accepting the first asset as payment in an event that the user and the issuer
16 are verified; and

17 subsequently passing any additional assets from the stick as payment to the
18 vendor without digitally signing them with the user's signature;

19
20 Claim 6 (Original): A method comprising:

21 minting a stick of electronic assets by digitally signing with an issuer's
22 signature a composite of user-provided data items including a user identity, a
23 bottom asset from a bottom of the stick, and a length of the stick;

24 spending one or more assets from the stick at one or more vendors, wherein
25 each expenditure with a particular vendor involves digitally signing with a user's

1 signature a first asset from the stick to be spent and passing the user-signed first
2 asset along with the issuer-signed composite to the particular vendor for
3 verification and subsequently passing any additional assets to be spent without user
4 signature to the particular vendor; and

5 depositing one or more assets collected by the particular vendor by digitally
6 signing with the particular vendor's signature a composite of data items including
7 the user-signed first asset and a last asset spent by the user from the stick and
8 passing the vendor-signed composite along with the issuer-signed composite to the
9 issuer, wherein the depositing comprises:

10 concatenating the user-signed first asset $S_U(C_j)$, a last asset spent from the
11 stick C_k , and a run length RL of assets beginning with the first asset C_j and ending
12 with the last asset C_k to form a deposit request;

13 signing the deposit request with a signature of the vendor:

$$S_V(S_U(C_j), C_k, RL)$$

14
15
16
17 submitting the vendor-signed deposit request along with the issuer-signed
18 withdrawal request to the issuer; and

19 crediting a vendor account with the run of assets in an event that the user,
20 the vendor, the run, and the issuer are positively verified.

21
22 Claim 7 (Original): A method as recited in claim 1, further comprising
23 auditing the assets deposited by the vendor.

24

25

1 Claim 8 (Original): A method as recited in claim 1, further comprising
2 auditing a sample of the assets paid by the user to the vendor.

3
4 Claim 9 (Original): A method as recited in claim 1, further comprising
5 selecting, at the vendor, a subset of less than all of the assets paid by the user to the
6 vendor and submitting the subset of assets to an auditor for fraud evaluation.

7
8 Claim 10 (Original): Distributed computer-readable media resident at the
9 issuer, user, and vendor having computer-executable instructions to perform the
10 method as recited in claim 1.

11
12 Claim 11 (Original): Computers resident at the issuer, user, and vendor that
13 are programmed to perform the method as recited in claim 1.

14
15 Claim 12 (Original): A method for issuing electronic assets, comprising:
16 forming a stick of L electronic assets C_i (for $i=1, \dots, L$) where each asset
17 can be derived from a preceding asset in the stick;
18 signing the stick with a signature of a party issuing the assets;
19 spending a first run of one or more assets from the stick at a first vendor;
20 and
21 spending a second run of one or more assets from the stick at a second
22 vendor.

1 Claim 13 (Original): A method as recited in claim 12, further comprising
2 storing the stick of electronic assets in a tamper-resistant electronic wallet.

3
4 Claim 14 (Original): A method as recited in claim 12, further comprising
5 storing the stick of electronic assets in an electronic wallet constructed with a
6 secure-processor architecture.

7
8 Claim 15 (Original): A method as recited in claim 12, wherein the forming
9 comprises anonymously issuing the stick of assets using a blind signature protocol.

10
11 Claim 16 (Original): A method as recited in claim 12, wherein the forming
12 comprises:

13 creating the stick of L electronic assets by computing:

$$14 \quad C_i = h^i(x) \quad (\text{for } i=1, \dots, L)$$

15
16
17 where $h(x)$ is a one-way hashing function of a value x .

18
19 Claim 17 (previously amended): A method for issuing electronic assets,
20 comprising:

21 forming a stick of L electronic assets C_i (for $i=1, \dots, L$) where each asset
22 can be derived from a preceding asset in the stick; wherein the forming comprises:

23 creating the stick of L electronic assets by computing:

$$24 \quad C_i = h^i(x) \quad (\text{for } i=1, \dots, L)$$

where $h(x)$ is a one-way hashing function of a value x ;

constructing a withdrawal request having a user identity U , a user secret K , a last asset value C_L taken from a bottom of the stick, a denomination d indicating a value for the assets in the stick, an expiration t , and the value L ; and

signing the withdrawal request with a signature of an issuer:

$$S_I(U, K, d, C_L, t, L);$$

signing the stick with a signature of a party issuing the assets;

spending a first run of one or more assets from the stick at a first vendor;

and

spending a second run of one or more assets from the stick at a second vendor.

Claim 18 (Original): A method as recited in claim 12, wherein the spending comprises:

signing a first asset from the stick with a signature of the user:

submitting the user-signed asset along with the signed stick to the first vendor; and

in an event the first asset is accepted, subsequently submitting any additional assets from the stick without digitally signing them.

1 Claim 19 (Original): A method as recited in claim 12, further comprising
2 auditing the assets from the first and second runs of assets for fraud.

3
4 Claim 20 (Original): A method as recited in claim 12, further comprising
5 auditing a sample of assets from the first and second runs of assets for fraud.

6
7 Claim 21 (Original): A method as recited in claim 12, further comprising
8 depositing the first and second runs of assets.

9
10 Claims 22-23 (Canceled)

11
12 Claim 24 (Original): A method for issuing electronic assets, comprising:
13 creating, at a user, a stick of L electronic assets by computing:

$$14 \quad C_i = h^i(x) \quad (\text{for } i=1, \dots, L)$$

15
16
17 where $h(x)$ is a hashing function of a value x ;

18 submitting a withdrawal request from the user to an issuer, the withdrawal
19 request having a user identity U , a last asset value C_L taken from a bottom of the
20 stick, and the value L , while omitting any vendor identity;

21 signing, at the issuer, the withdrawal request; and

22 returning the signed withdrawal request to the user.
23
24
25

1 Claim 25 (Original): A method as recited in claim 24, further comprising
2 storing the stick of electronic assets and signed withdrawal request in a tamper-
3 resistant electronic wallet.

4
5 Claim 26 (Original): A method as recited in claim 24, further comprising
6 storing the stick of electronic assets and signed withdrawal request in an electronic
7 wallet constructed with a secure-processor architecture.

8
9 Claim 27 (Original): A method as recited in claim 24, wherein the
10 withdrawal request further has a user secret K , a denomination d indicating a value
11 for the assets in the stick, and an expiration t .

12
13 Claims 28-30 (Canceled)

14
15 Claim 31 (Original): A method comprising:
16 creating, at a user, a stick of L electronic assets by computing:

17
18
$$C_i = h^i(x) \text{ (for } i=1, \dots, L)$$

19
20 where $h(x)$ is a hashing function of a value x ;

21 submitting a withdrawal request from the user to an issuer, the withdrawal
22 request having a user identity U , a user secret K , a last asset value C_L taken from a
23 bottom of the stick, a denomination d indicating a value for the assets in the stick,
24 an expiration t , and the value L ;

25 signing, at the issuer, the withdrawal request:

$$S_I(U, K, d, C_L, t, L)$$

returning the issuer-signed withdrawal request to the user;
initiating payment of one or more assets from the stick to a vendor having
an identity V ;
concatenating, at the user, the vendor identity with a first asset C_j to be
spent from the stick to form a payment request, and a depth D indicating a distance
of the first asset from the bottom of the stick;
signing the payment request with a signature of the user:

$$S_U(C_j, D, VI)$$

submitting the user-signed payment request along with the issuer-signed
withdrawal request to the vendor;
accepting the first asset as payment at the vendor in an event that the user
and the issuer are verified;
subsequently passing any additional assets from the stick as payment to the
vendor without digitally signing them with the user's signature;
concatenating, at the vendor, the user-signed first asset, a last asset spent
from the stick C_k , and a run length RL of assets beginning with the first asset C_j
and ending with the last asset C_k to form a deposit request;
signing the deposit request with a signature of the vendor:

$$S_V(S_U(C_j), C_k, RL)$$

1
2 submitting the vendor-signed deposit request along with the issuer-signed
3 withdrawal request to the issuer; and

4 crediting a vendor account with the run of assets in an event that the user,
5 the vendor, and the issuer are verified.
6

7 Claim 32 (Original): A method as recited in claim 31, further comprising
8 randomly selecting an asset from the assets paid by the user to the vendor and
9 submitting the selected asset for audit.
10

11 Claim 33 (Original): A method as recited in claim 31, further comprising
12 auditing the assets deposited by the vendor with the issuer.
13

14 Claim 34 (Original): A method for anonymously issuing electronic assets,
15 comprising:

16 creating, at a user, a stick of L electronic assets by computing:
17

$$18 \quad C_i = h^i(x) \quad (\text{for } i=1, \dots, L)$$

19
20 where $h(x)$ is a hashing function of a value x ;

21 blinding the stick using a random value p , where:
22

$$23 \quad \text{Blind Stick} = p^e C_L \bmod N$$

24
25 where C_L is a bottom asset on the stick;

1 submitting a withdrawal request from the user to an issuer, the withdrawal
2 request having the blind stick and the value L ;

3 signing, at the issuer, the withdrawal request by computing:

$$c = (p^e C_D)^{L_f} = p^L C_L^{L_f} \bmod N$$

4
5
6
7 where e and f are public and private variables known by the issuer and e is
8 known to everyone;

9 returning the signed withdrawal request to the user;

10 deriving a new bottom asset by computing:

$$C_L^{L_f} = c/p^L \bmod N.$$

11
12
13
14 Claim 35 (Original): A method as recited in claim 34, further comprising
15 storing the blind stick of electronic assets and signed withdrawal request in a
16 tamper-resistant electronic wallet.

17
18 Claim 36 (Original): A method as recited in claim 34, further comprising
19 verifying the bottom asset by computing $C_L^{L_f}$ independently and comparing a result
20 to the new bottom asset derived in said deriving ($C_L^{L_f}$)

21
22 Claim 37 (Original): A method as recited in claim 34, further comprising
23 storing the blind stick of electronic assets and signed withdrawal request in an
24 electronic wallet constructed with a secure-processor architecture.

25

1 Claim 38 (Original): A method as recited in claim 34, further comprising
2 spending an asset from the blind stick by first sending the new bottom to a vendor
3 for verification.

4
5 Claims 39-41 (Canceled)

6
7 Claim 42 (Withdrawn): A method for handling electronic coupons,
8 comprising:

9 creating dual sticks of corresponding coupons including a user stick located
10 at the user and a vendor stick located at the vendor;

11 referencing at least one coupon in the user stick and at least one
12 corresponding coupon in the vendor stick;

13 upon granting or spending a coupon, changing reference to a different
14 coupon in the user stick and a different corresponding coupon in the vendor stick;
15 and

16 swapping information between the user and the vendor to verify that the
17 coupons being referenced in the user stick and the vendor stick correspond to one
18 another.

19
20 Claim 43 (Withdrawn): A method as recited in claim 42, wherein the
21 referencing comprises:

22 using a first user pointer to reference a newest coupon in the user stick and
23 a second user pointer to reference an oldest unused coupon in the user stick; and
24
25

1 using a first vendor pointer to reference a newest coupon in the vendor stick
2 and a second vendor pointer to reference an oldest unused coupon in the vendor
3 stick.

4
5 Claim 44 (Withdrawn): A method as recited in claim 43, wherein the
6 changing comprises, upon granting a newer coupon, moving the first user pointer
7 and the first vendor pointer to reference the newer coupon.

8
9 Claim 45 (Withdrawn): A method as recited in claim 43, wherein the
10 changing comprises, upon spending the oldest coupon, moving the second user
11 pointer and the second vendor pointer to reference a next oldest coupon.

12
13 Claim 46 (Withdrawn): A method as recited in claim 42, wherein the
14 swapping comprises exchanging data indicating which coupons are being
15 referenced in the user stick and the vendor stick.

16
17 Claim 47 (Withdrawn): Computer-readable media resident at the user
18 and the vendor having computer-executable instructions that perform the method
19 as recited in claim 42.

20
21 Claim 48 (Withdrawn): Computers resident at the user and the vendor
22 that are programmed to perform the method as recited in claim 42.

23
24 Claim 49 (Withdrawn): A method for handling electronic coupons,
25 comprising:

1 storing a first set of coupons in a user-based data structure maintained at a
2 user;
3 storing a second set of coupons in a vendor-based data structure maintained
4 at a vendor, the second set of coupons corresponding to the first set of coupons;
5 using first and second user pointers to reference a first and last coupon in
6 the user-based data structure;
7 using first and second vendor pointers to reference a first and last coupon in
8 the vendor-based data structure;
9 upon earning a new coupon,
10 adding the new coupon to the user-based stick;
11 modifying the first user pointer at the user-based data structure to reflect the
12 new coupon;
13 informing the vendor;
14 updating the first vendor pointer at the vendor-based data structure to reflect
15 that the user-based data structure is referencing the new coupon;
16 upon spending a current coupon from the user-based data structure,
17 submitting the current coupon to the vendor;
18 evaluating, at the vendor, whether the coupon is acceptable and if
19 acceptable, modifying the second pointer at the vendor-based data structure to
20 reflect expenditure of the coupon;
21 informing the user;
22 updating the second user pointer at the user-based data structure to reflect
23 expenditure of the current coupon.
24
25

1 Claim 50 (Withdrawn): An architecture for managing electronic
2 coupons, comprising:

3 a user-based data structure embodied on a computer-readable medium, the
4 user-based data structure storing one or more coupons;

5 a first user pointer to an oldest coupon in the user-based data structure;

6 a second user pointer to a newest coupon in the user-based data structure;

7 a vendor-based data structure embodied on a computer-readable medium,
8 the vendor-based data structure storing one or more coupons associated with the
9 coupons stored on the user-based data structure;

10 a first vendor pointer to an oldest coupon in the vendor-based data
11 structure;

12 a second vendor pointer to a newest coupon in the vendor-based data
13 structure;

14 wherein the user-based data structure and the vendor-based data structure
15 are concurrently maintained so that (1) modification of the first user pointer to
16 reference another coupon in the user-based stick results in updating and
17 verification of the first vendor pointer to reference an associated coupon in the
18 vendor-based stick and (2) modification of the second vendor pointer to reference
19 a different coupon in the vendor-based stick results in updating and verification of
20 the second user pointer to reference an associated coupon in the user-based stick.

21
22
23 Claim 51 (Original): An electronic asset system comprising:

24 an issuer wallet having a processor and storage, the issuer wallet digitally
25 signing with an issuer's signature a composite of user-provided data items

1 including a user identity, a bottom asset from a bottom of a stick of electronic
2 assets, and a length of the stick;

3 a user wallet having a processor and storage to store the stick of electronic
4 assets and issuer-signed composite and to spend one or more assets from the stick
5 at one or more vendors, the user wallet spending one or more assets by digitally
6 signing with a user's signature a first asset from the stick to be spent and passing
7 the user-signed first asset along with the issuer-signed composite to the vendor for
8 verification; whereupon verification, the user wallet subsequently passes any
9 additional assets to be spent without user signature to the vendor; and

10 a vendor wallet having a processor and storage to store one or more assets
11 spent by the user wallet, the vendor wallet depositing the assets collected from the
12 user wallet by digitally signing with the particular vendor's signature a composite
13 of data items including the user-signed first asset and a last asset passed in the
14 stick received from the user wallet and passing the vendor-signed composite along
15 with the issuer-signed composite to the issuer wallet for verification.

16
17 Claim 52 (Original): An electronic asset system as recited in claim 51,
18 wherein the issuer wallet, the user wallet, and the vendor wallet are tamper-
19 resistant.

20
21 Claim 53 (Original): An electronic asset system as recited in claim 51,
22 wherein the issuer wallet, the user wallet, and the vendor wallet are tamper-
23 resistant constructed with a secure-processor architecture.

24
25

1 Claim 54 (Original): An electronic asset system as recited in claim 51,
2 wherein the issuer wallet signs the composite using a blind signature protocol.

3
4 Claim 55 (Original): An electronic asset system as recited in claim 51,
5 further comprising an auditing system to audit the electronic assets to detect
6 whether assets have been used in a fraudulent manner.

7
8 Claim 56 (Original): An electronic asset system as recited in claim 51,
9 further comprising a probabilistic auditing system to sample a subset of less than
10 all electronic assets to detect whether assets have been used in a fraudulent
11 manner.

12
13 Claim 57 (Original): An electronic wallet having memory and a processor,
14 the electronic wallet being programmed to:
15 create a stick of L electronic assets by computing:

$$16 \quad C_i = h^i(x) \text{ (for } i=1, \dots, L)$$

17
18
19 where $h(x)$ is a hashing function of a value x ;

20 form a withdrawal request having a user identity U , a last asset value C_L
21 taken from a bottom of the stick, and the value L , while omitting any vendor
22 identity;

23 submit withdrawal request to an issuer and receive the withdrawal request
24 back with an issuer signature; and

25 store the signed withdrawal request and the stick.

1
2 Claim 58 (Original): An electronic wallet having memory and a processor,
3 the electronic wallet being programmed to:

4 create a stick of L electronic assets by computing:

$$5 \\ 6 \quad C_i = h^i(x) \quad (\text{for } i=1, \dots, L)$$

7
8 where $h(x)$ is a hashing function of a value x ;

9 form a withdrawal request having a user identity U , a last asset value C_L
10 taken from a bottom of the stick, and the value L , while omitting any vendor
11 identity;

12 submit withdrawal request to an issuer and receive the withdrawal request
13 back with an issuer signature;

14 store the signed withdrawal request and the stick;

15 form a payment request for payment of one or more assets from the stick to
16 a vendor having an identity V , the payment request having the vendor identity V
17 and a first asset C_j to be spent from the stick;

18 sign the payment request:

$$19 \\ 20 \quad S_U(C_j, V); \text{ and}$$

21
22 submit the signed payment request along with the signed withdrawal
23 request to the vendor.

24
25 Claims 59-60 (Canceled).